Smart Grid Interoperability Panel - Cyber Security Working Group Standards Review

Phase 1 Report

October 7, 2010

Acknowledgements

I would like to acknowledge the hard work and dedication of the Cyber Security Working Group (CSWG) Standards Subgroup and the Co-leads, Virginia Lee and Frances Cleveland for reviewing the standards and providing a quality product. Also, I would like to recognize Victoria Yan, Booz Allen Hamilton for the many late nights compiling this report and keeping the group on track. Lastly, I would like to thank my NIST colleagues, Tim Polk and Kelley Dempsey for reviewing the document and providing valuable comments.

Marianne Swanson
Chair, Cyber Security Working Group

Table of Contents

1. Introduction

1.1 Correlation of Cyber Security with Communication Standards

Correlating cyber security with specific communication standards is very complex and is not a one-to-one correlation.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the communications "stack" or "profile." Some standards address the lower layers of the stack, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cyber security technologies cannot be linked to them until they are translated into "bits and bytes" by mapping them to one of the semantic structures.

Secondly, regardless of what communications standards are used, cyber security must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cyber security must address many aspects outside of the communications system that typically rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cyber security must also address how to: cope during an attack, recover from it afterwards, and create a trail of information to be used in post-attack analysis.

Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data.

Therefore, cyber security must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of communication standards designed to provide specific services. Ultimately, cyber security as applied to these stacks of communication standards should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cyber security technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used. For some specific Smart Grid communication standards, such as International Eletrotechnical Commission (IEC) 61850 and IEC 60870-6, specific cyber security standards (IEC 62351 series) were developed to meet typical implementations of these standards.

In the following discussions of communication standards, these caveats should be taken into account.

1.2 Standardization Cycles of Communication Standards

Communication standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cyber security requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cyber security has become increasingly important within the utility sector. However, since the development cycles of communication standards and cyber security standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references will be added.

Since technologies (including cyber security technologies) are rapidly changing to meet increasing new and more powerful threats, some cyber security standards can be out-of-date by the time they are released. This means that some minimum requirements may be considered too weak while references to other security standards may be rapidly obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

2. IEC 60870-6/TASE.2/ICCP: Control Center to Control Center Information Exchanges

2.1 Description of Communications Standard

IEC 60870-6 (also known as Telecontrol Application Service Element (TASE.2) and Inter-Control Center Communications Protocol (ICCP)) is an "application layer" communication standard that defines message structures, some very basic object structures, and profiles of communication standards to be used within the transport layers. The primary objective of IEC 60870-6 is to provide control center to control center data exchanges, but it has been applied to other domains with comparable requirements. Examples of such domains include: power plants, factory automation, and process control automation.

IEC 60870-6/TASE.2 consists of three key documents: 1) IEC 60870-6-503 defines the TASE.2 application modeling and service definitions; 2) IEC 60870-6-702 defines the application profile for use with TASE.2; and 3) IEC 60870-6-802 defines a set of standardized object definitions to be supported. A User Guide (IEC 60870-6-505) was also developed as a Technical Report.

2.1.1 IEC 60870-6-503: TASE.2 Services and Protocol

IEC 60870-6-503 specifies a method of exchanging time-critical control center data across wide-area and local-area networks using a full International Organization for Standardization (ISO) compliant protocol stack. It contains provisions for supporting both centralized and distributed architectures. This standard includes the exchange of real-time data indications, control operations, time-series data, scheduling and accounting information, remote program control, and event notification.

2.1.2 IEC 60870-6-702: Functional Profile for Providing the TASE.2 Application Service in End Systems

This standard consists of a functional profile (FP) and defines the provision of the TASE.2 communications services between two control center end systems. This FP also defines the provision of the OSI connection-mode presentation and session services between the end systems.

2.1.3 IEC 60870-6-802: TASE.2 Object Models

The primary purpose of TASE.2 is to transfer data between control systems and to initiate control actions. This defines a method of exchanging time-critical control center data through both wide-area networks and local-area networks using a fully ISO-compliant protocol stack, supporting both centralized and distributed architectures. Data is represented by object instances. IEC 60870-6-802 proposes object models from which to define object instances. The object models represent objects for transfer. The local system may not maintain a copy of every attribute of an object instance.

2.1.4 IEC TR 60870-6-505 Amend 1: TASE.2 User Guide

This report provides guidance for utility users who are evaluating, procuring, and configuring TASE.2, as well as aid to vendors implementing TASE.2 in their products.

The individual server and data objects comprising TASE.2 are described, with cross references to the specification. This provides the reader the basic understanding needed to use the TASE.2 specifications in an informed manner. The guide then addresses practical issues that arise in connection with TASE.2 use. Clause 16 and Annex B provides a set of security informative guidelines on the use of the following TASE.2 international standards—

- IEC 60870-6-503, TASE.2 Services and Protocol,
- IEC 60870-6-702, TASE.2 Application Profiles, and
- IEC 60870-6-802, TASE.2 Object Models.

2.2 Summary of Cyber Security Content

2.2.1 Does the standard address cyber security? If not, should it?

The IEC 60870-6 series covers appropriate aspects of cyber security for the "application layer," but does not provide mechanisms for authorization or for encryption that would normally be provided by lower layer protocols.

IEC 60870-6-503 provides cyber security through access control between two control centers by establishing Bilateral Tables that identify those individual data elements in one control center that are allowed to be accessed by the other control center. These Bilateral Tables are established between control centers through legal bilateral agreements. Additional security is provided by reference in the IEC 60870-6-505 User Guide, Clause 16, and in Annex B.

The standard does not reference IEC 62351 because it was developed prior to it. However, IEC 62351, which covers security of communication protocols defined by IEC TC 57, does reference the 60870-6 series: "The scope of the IEC 62351 series is information security for power system control operations. The primary objective is to undertake the development of standards for security of the communication protocols defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series."

It is recommended that the IEC 60870-6 family be updated to reference IEC 62351.

2.2.2 What aspects of cyber security does the standard address, and how well (correctly) does it do so?

IEC 608070-6-503 describes the function of bilateral tables, which provide a rudimentary form of access control by requiring each source of information to first develop off-line (legally-binding) bilateral agreements with each receiver of information. These agreements are then implemented into bilateral tables, which must be used to check if the information requested by the receiver is authorized by the source's bilateral table. The bilateral tables are a key element of the enforcement mechanism. If the requester and the requested information are not identified in the applicable bilateral table, the requested information is not provided. Only data authentication is provided, not authentication of the source or receiver.

Bilateral tables are described in IEC 608070-6-503 clause 5.1.2: *bilateral agreements, bilateral tables and access control*, with the following references on ensuring the use of these bilateral agreements and tables—

- 5.2.1 General Access Control Requirements,
- 5.2.3 Bilateral Tables,
- 5.2.4 List of Access Control Specification, numerous other places within 5.2 that implement the requirements of 5.2.4 for various objects, and
- 6.4 Bilateral Table Object Model Mapping, numerous other places within Clause 6 referencing data defined in 6.4, and at numerous places in IEC 60870-6-503, Clause 7, Mapping of TASE.2 Operations and Actions onto MMS Services.

The applicable NIST Interagency Report (NISTIR) 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Access Control (SG.AC)	SG.AC-5, Information Flow Enforcement SG.AC-7, Least Privilege
Identification and Authentication (SG.IA)	SG.IA-3, Authenticator Management

The NISTIR 7628 high-level requirements do not include explicit access control of individual data elements, as defined in the bilateral table requirements. This may indicate a need for updates to the NISTIR 7628 high-level requirements.

Other applicable NISTIR 7628 high-level requirements are met through IEC 62351, Parts 3 and 5. For further detail on those clauses refer to the standards review of IEC 62351. The standard does not currently reference IEC 62351 because it was developed prior to it.

2.2.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

The IEC 62351 series covers certain aspects of cyber security of the communications protocols defined by IEC TC 57, including IEC 60870-6. All parts of IEC 62351 were published after the most recent final editions of IEC 60870-6, so that no normative references are made in IEC 60870-6 to IEC 62351.

It is recommended that the standards in the IEC 60870-6 family be updated to include normative references to the applicable parts of IEC 62351 during their review cycles.

The source and receiver are not authenticated, only the data is checked to determine who is allowed to access it. However, authentication of source and receiver should be covered by IEC 62351-8, which is expected to become a standard within the next year.

No other types of security (aside from bilateral tables addressing partial access control) are covered in this standard – the additional security requirements for user authentication are covered in IEC 62351, Part 3, Clause 5 and IEC 62351, Part 4, Clauses 5-6 (see those reviews for further detail). Role-based access control will be addressed by IEC 62351-8.

Cryptography is also not included in the standard, nor should it be. Cryptography for IEC 60870-6 is addressed in IEC 62351, Parts 3 and 4.

2.2.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

A reference to IEC 62351 regarding cryptography is planned to be incorporated into IEC 60870-6-505 (User Guide), which currently addresses other aspects of security (see Section 2.2.2). No timeframe for completion has been noted.

IEC 60870-6-702, Annex B describes future developments in security, network management, and performance. Specific topics for future development include:

- Network layer security protocol,
- Transport layer security protocol,
- Mechanisms for implementing application requirements in the networks (e.g., priority, high-speed transport protocols),
- Security application service element,
- Access control in ACSE, and
- Definition of managed objects at all layers.

2.2.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed.

The following standards are normative as described in 60870-6-2:

- CEPT T/CD 01-12, *Specifications for engineering requirements for 3 types of plug-in DCE's operating with a use data signaling rate of 2400 bits/s*
- CEPT T/CD 01-14, *Specifications of equipment practice for data transmission equipment*
- IEC 50(371): 1984, *International Electrotechnical Vocabulary (IEV) - Chapter 371: Telecontrol*
- IEC 50(721): 1991, *International Electrotechnical Vocabulary (IEV) - Chapter 721: Telegraphy, facsimile and data communication*
- IEC 870-1-3: 1990, *Telecontrol equipment and systems - Part 1: General considerations - Section3: Glossary*
- IEC 870-6-1: 1994, *Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - Section 1: Application context and organization of standards*
- ISO 2110: 1989, *Information technology - Data communication - 25-pole DTE/DCE interface connector and contact number assignments*
- ISO 2382-9: 1984, *Data processing - Vocabulary - Part 09: Data communication*
- ISO 4903: 1989, *Information technology - Data communication - 15-pole DTE/DCE interface connector and contact number assignments*
- ISO 7776: 1986, *Information processing systems - Data communications - High-level data link control procedures - Description of the X.25 LAPB-compatible DTE data link procedures*
- ISO 8602: 1987, *Information processing systems - Open Systems Interconnection - Protocol for providing the connectionless-mode transport service*

- ISO 8648: 1988, *Information processing systems - Open Systems Interconnection - Internal organization of the Network Layer*
- ISO 8802-2: 1992, *Information processing systems - Local area networks - Part 2: Logical link control*
- ISO/IEC 10022: 1990, *Information technology - Open Systems Interconnection - Physical Service Definition*
- ISO/IEC 3309: 1993, *Information technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures - Frame structure*
- ISO/IEC 4335: 1993, *Information technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures - Elements of procedures*
- ISO/IEC 7489-1: 1994, *Information technology - Open Systems Interconnection - Reference Model - Part1: Basic Reference Model*
- ISO/IEC 7809: 1993, *Information Technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures - Classes of procedures*
- ISO/IEC 8072: 1994, *Information technology - Open Systems Interconnection - Transport service definition*
- ISO/IEC 8073: 1992, *Information technology - Telecommunications and information exchange between systems - Open Systems Interconnection - Protocol for providing the connection-mode transport service*
- ISO/IEC 8208: 1990, *Information technology - Data communications - X.25 Packet Layer Protocol for Data Terminal Equipment*
- ISO/IEC 8348: 1993, *Information technology - Open Systems Interconnection - Network service Definition*
- ISO/IEC 8473-1: 1994, *Information technology - Protocol for providing the connectionless-mode network service: Protocol specification*
- ISO/IEC 8878: 1992, *Information technology - Telecommunications and information exchange between systems - Use of X.25 to provide the OSI Connection-Mode Network Service*
- ISO/IEC 8880-2: 1992, *Information technology - Telecommunications and information exchange between systems - Protocol combinations to provide and support the OSI Network Service - part 2: Provision and support of the connection-mode Network Service*
- ISO/IEC 8880-3: 1990, *Information Technology - Telecommunications and information exchange between systems - Protocol combinations to provide and support the OSI Network Service - part 3: Provision and support of the connectionless-mode Network Service*
- ISO/IEC 8886: 1992, *Information technology - Telecommunications and information exchange between systems - Data link service definition for Open System Interconnection*
- ISO/IEC TR 10172: 1991, *Information technology - Telecommunications and information exchange between systems - Network Transport Protocol interworking specification*
- ITU-T T.5009: 1992, *International Reference Alphabet*
- ITU-T V.10: 1993, *Electrical characteristics for unbalanced double-current interchange circuits operating at data signaling rates nominally up to 100 kbits/s*
- ITU-T V.11: 1993, *Electrical characteristics for unbalanced double-current interchange circuits operating at data signaling rates up to 10 Mbits/*s

- ITU-T V.21: 1988, *300 bits per second duplex modem standardized for use in the general switched telephone network*
- ITU-T V.22, 1988, *1200 bits per second duplex modem standardized for use in the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits*
- ITU-T V.22bis: 1988, *2400 bits per second duplex modem using the frequency division technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits*
- ITU-T V.23: 1988, *600/1200-baud model standardized for use in the general switched telephone network*
- ITU-T V.24: 1993, *List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)*
- ITU-T V.25: 1988, *Automatic answering equipment and/or parallel automatic calling equipment on the general switched telephone network including procedures for disabling of echo control devices for both manually and automatically established calls*
- ITU-T V.25bis: 1988, *Automatically calling and/or answering equipment on the general switched telephone network (GSTN) using the 100-series interchange circuits*
- ITU-T V.26bis: 1988, *2400/1200 bits per second modem standardized for use in the general switched telephone network*
- ITU-T V.26ter: 1988, *2400 bits per second duplex modem using the echo cancellation technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits*
- ITU-T V.27: 1988, *4800 bits per second modem with manual equalizer standardized for use on leased telephone-type circuits*
- ITU-T V.28: 1993, *Electrical characteristics for unbalanced double-current interchange circuits*
- ITU-T V.31: 1988, *electrical characteristics for single-current interchange circuits controlled by contact closure*
- ITU-T V.31bis: 1988, *Electrical characteristics for single-current interchange circuits using optocouplers*
- ITU-T V.32: 1993, *A family of 2-wire, duplex modems operating at data signaling rates of up to 9600 bits/s for use on the general switched telephone network and on leased telephone-type circuits*
- ITU-T X.21: 1992, *Interface between data terminal equipment and data circuit-terminating equipment for synchronous operation on public data networks*
- ITU-T X.211: 1988 (ISO 10022), *Physical service definition for open system interconnection for ITU-T applications*
- ITU-T X.212: 1988 (ISO 8886), *Data link service definition for open systems interconnection for ITU-T applications*
- ITU-T X.213: 1992 (ISO 8348), *Information technology - Network service definition for Open Systems Interconnection*
- ITU-T X.21bis: 1988, *Use on public data networks of data terminal equipment (DTE) which is designed for interfacing to synchronous V-Series modems*
- ITU-T X.24: 1988, *List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) on public data networks*
- ITU-T X.25: 1993, *Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit*

- ITU-T X.26: 1988, *Electrical characteristics for unbalanced double-current interchange circuits for general use with integrated circuit equipment in the field of data communications*
- ITU-T X.27: 1988, *Electrical characteristics for balanced double-current interference circuits for general use if integrated circuit equipment in the field of data communications*
- ITU-T X.4: 1988, *General structure of signals on International Alphabet No. 5 code for character oriented data transmission over public data networks*
- ITU-T X.75: 1993, *Packet-switched signaling system between public networks providing data transmission services*

The following standards are normative as described in 60870-6-501:

- IEC 870-6-502: 1995, *Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and IUT-T recommendations - Section 502: TASE.1 Protocol definitions*
- ISO 7498: 1984, *Information processing systems - Open Systems Interconnection - Basic Reference Model*
- ISO 7498-3: 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 3: Naming and addressing*
- ISO 8649, 1988, *Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element*
- ISO 8650: 1988, *Information processing systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element*
- ISO 8822: 1994, *Information technology - Open Systems Interconnection - Presentation service definition*
- ISO/IEC 8824: 1990, *Information technology - Open Systems Interconnection - Specification of the Abstract Syntax Notation One (ASN.1)*
- ISO/IEC 9072-1: 1989, *Information processing systems - Text communication - Remote Operations - Part 1: Model notation and service definition*
- ISO/IEC 9072-2: 1989, *Information processing systems - Text communication - Remote Operations - Part 2: Protocol specification*
- ISO/TR 8509: 1987, *Information processing systems - Open Systems Interconnection - Service conventions*

The following standards are normative as described in 60870-6-502:

- IEC 870-6-501: 1995, *Telecontrol equipment and systems - part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - Section 501: TASE.1 service definitions*
- ISO 7498: 1984, *Information processing systems - Open Systems Interconnection - Basic Reference Model*
- ISO 8649, *Information processing systems. Open Systems Interconnection. Service definition for the Association Control Service Element*
- ISO 8650: 1988, *Information processing systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element*
- ISO 8822: 1994, *Information technology - Open Systems Interconnection - Presentation service definition*
- ISO 8859-1: 1987, *Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin Alphabet No. 1*

- ISO/DIS 8825-2*, *Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 2: Packed encoding rules*
- ISO/IEC 8824: 1990, *Information technology - Open Systems Interconnection - Specification of the Abstract Syntax Notation One (ASN.1)*
- ISO/IEC 8825: 1990, *Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*
- ISO/IEC 9072-1: 1989, *Information processing systems - Text communication - Remote Operations - Part 1: Model notation and service definition*
- ISO/IEC 9072-2: 1989, *Information processing systems - Text communication - Remote Operations - Part 2: Protocol specification*
- ISO/TR 8509: 1987, *Information processing systems - Open Systems Interconnection - Service conventions*

The following standards are normative as described in 60870-6-503:

- IEC 60870-6-702:1998, *Telecontrol equipment and systems. Part 6-702: Telecontrol protocols compatible with ISO standards and ITU-T recommendations. Functional profile for providing the TASE.2 application service in end systems*
- IEC 60870-6-802:2002, *Telecontrol equipment and systems. Part 6-802: Telecontrol protocols compatible with ISO standards and ITU-T recommendations. TASE.2 Object models*
- ISO 8649, *Information processing systems. Open Systems Interconnection. Service definition for the Association Control Service Element*
- ISO 9506-1:2000, *Industrial automation systems. Manufacturing Message Specification. Part 1: Service definition*
- ISO 9506-2:2000, *Industrial automation systems. Manufacturing Message Specification. Part 2: Protocol specification*
- ISO/IEC 10589:1992, *Information technology. Telecommunications and information exchange between systems. Intermediate system to intermediate system intra-domain-routing exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network Service (ISO 8473)*
- ISO/IEC 8073, *Information technology. Open Systems Interconnection. Protocol for providing the connection-mode transport service*
- ISO/IEC 8208:2000, *Information technology. Data communications. X.25 Packet Layer Protocol for Data Terminal Equipment*
- ISO/IEC 8473, *Information technology. Protocol for providing the connectionless-mode network service*
- ISO/IEC 8802-3:2001, *Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*
- ISO/IEC 9542, *Information processing systems. Telecommunications and information exchange between systems. End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*
- ISO/IEC ISP 10608-1:1992, *Information technology. International Standardized Profile TAnnnn. Connection-mode Transport Service over Connectionless-mode Network Service. Part 1: General overview and subnetwork-independant requirements*

- ISO/IEC ISP 10608-2:1992, *Information technology. International Standardized Profile TAnnnn. Connection-mode Transport Service over Connectionless-mode Network Service. Part 2: TA51 profile including subnetwork-dependent requirements for CSMA/CD Local Area Networks (LANs)*
- ISO/IEC ISP 10608-5:1992, *Information technology. International Standardized Profile TAnnnn. Connection-mode Transport Service over Connectionless-mode Network Service. Part 5: TA1111/TA1121 profiles including subnetwork-dependent requirements for X.25 packet switched data networks using virtual calls*
- ISO/IEC ISP 10613-1:1994, *Information technology. International Standardized Profile RA. Relaying the Connectionless-mode Network Service. Part 1: Subnetwork-independent requirements*
- ISO/IEC ISP 10613-2:1994, *Information technology. International Standardized Profile RA. Relaying the Connectionless-mode Network Service. Part 2: LAN Subnetwork-dependent, media-independent requirements*
- ISO/IEC ISP 10613-3:1994, *Information technology. International Standardized Profile RA. Relaying the Connectionless-mode Network Service. Part 3: CSMA/CD LAN subnetwork dependent, media-dependent requirements*
- ISO/IEC ISP 10613-5:1994, *Information technology. International Standardized Profile RA. Relaying the Connectionless-mode Network Service. Part 5: Definition of profile RA51.51, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks*
- ISO/IEC ISP 10613-7:1994, *Information technology. International Standardized Profile RA. Relaying the Connectionless-mode Network Service. Part 7: PSDN subnetwork-dependent, media-dependent requirements for virtual calls over a permanent access*
- ISO/IEC ISP 10613-8:1994, *Information technology. International Standardized Profile RA. Relaying the Connectionless-mode Network Service. Part 8: Definition of profile RA51.1111, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks and PSDNs using virtual calls over a PSTN leased line permanent access*
- ISO/IEC ISP 10613-9:1994, *Information technology. International Standardized Profile RA. Relaying the Connectionless-mode Network Service. Part 9: Definition of profile RA51.1121, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks and PSDNs using virtual calls over a digital data circuit/CSDN leased line permanent access*

The following standards are normative as described in 60870-6-601:

- 57/201/DIS, *Telecontrol equipment and systems - part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - Section 2: Use of base standards - Layers 1 to 4 (future IEC 870-6-2)*
- ISO 7776: 1986, *Information processing systems - Data communications - High-level data link control procedures - Description of the X.25 LAPB-compatible DTE data link procedures*
- ISO DIS 10588: 1992, *Information technology - Telecommunications and information exchange between systems - Use of X.25 Packet layer Protocol in conjunctions with X.21/X.21 bis to provide the OSI Connection-mode Network Service*
- ISO DIS 10732: 1992, *Information technology - Telecommunications and information exchange between systems - Use of X.25 Packet Layer Protocol to provide the OSI Connection-mode Network Service over the telephone network*
- ISO/IEC 8072: 1994, *Information technology - Open Systems Interconnection - Transport service definition*

- ISO/IEC 8073: 1992, *Information technology - Telecommunications and information exchange between systems - Open Systems Interconnection - Protocol for providing the connection-mode transport service*
- ISO/IEC 8208: 1990, *Information technology - Data communications - X.25 Packet Layer Protocol for Data Terminal Equipment; Amendment 3: 1991, Conformance requirements*
- ISO/IEC 8348: 1993, *Information technology - Open Systems Interconnection - Network service Definition*
- ISO/IEC 8878: 1992, *Information technology - Telecommunications and information exchange between systems - Use of X.25 to provide the OSI Connection-Mode Network Service*
- ISO/IEC ISP 10609-1: 1992, *Information technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over connection-mode Network Service - Part 1: Subnetwork-type independent requirements for Group TB*
- ISO/IEC ISP 10609-5: 1992, *Information technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over connection-mode Network Service - Part 5: Definition of profiles TB1111/TB1121*
- ISO/IEC ISP 10609-9: 1992, *Information technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over connection-mode Network Service - Part 9: Subnetwork-type dependent requirements for Network Layer, Data Link Layer and Physical Layer concerning permanent access to a packet switched data network using virtual calls*
- ISO/IEC TR 10029: 1989, *Information technology - Telecommunications and information exchange between systems - Operation of an X.25 interworking unit*
- ITU-T X.21: 1988, *Interface between data terminal equipment (DTE) and data-terminating equipment (DCE) for synchronous operation on public data networks (PDNs*)
- ITU-T X.21bis: 1988, *Use on PDNs of DTE which is designed for interfacing to synchronous V-series modems*
- ITU-T X.25: 1988, *Interface between DTE and DCE for terminals operating in the packet mode and connected to public data networks by dedicated circuit*

The following standards are normative as described in 60870-6-701:

- IEC 60870-6-502:1995, *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – Section 502: TASE.1 protocol definitions*
- ISO/IEC 8326:1987, *Information processing systems – Open Systems Interconnection – Basic connection oriented session service definition*
- ISO/IEC 8327:1987, *Information processing systems – Open Systems Interconnection – Basic connection oriented session protocol specification*
- ISO/IEC 8327-2:1996, *Information technologies – Open Systems Interconnection – Connection oriented session protocol – Protocol implementation conformance statement (PICS) proforma*
- ISO/IEC 8649:1996, *Information technologies – Open Systems Interconnection – Service definition for the Association Control Service Element (ACSE)*
- ISO/IEC 8650:1988, *Information processing systems – Open Systems Interconnection – Protocol Specification for the Association Control Service Element (ACSE)*

- ISO/IEC 8650-2:1995, *Information technology – Open Systems Interconnection – Protocol Specification for the Association Control Service Element – Protocol Implementation Conformance Statement (PICS) proforma*
- ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – Presentation service definition*
- ISO/IEC 8823:--, *Information technology – Open Systems Interconnection – Connection oriented presentation protocol*
- ISO/IEC 8823-2:1995, *Information technology – Open Systems Interconnection – Connection oriented presentation protocol – Protocol Implementation Conformance Statement (PICS) proforma*
- ISO/IEC 9072-2:1989, *Information processing systems – Text communication – Remote operations – Part 2: Protocols specification*

The following standards are normative as described in 60870-6-702:

- IEC 60870-6-503:1997, *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – Section 503: TASE.2 Services and protocol*
- ISO/IEC 8327-2:1996, *Information technologies – Open Systems interconnection – Connection oriented session protocol – Part 2: Protocol implementation conformance statement (PICS) proforma*
- ISO/IEC 8650-2:1997*, Information technology – Open Systems Interconnection – Protocol specification for the Association Control Service Element – Part 2: Protocol Implementation Conformance Statement (PICS) proforma*
- ISO/IEC 8823-2:1997, *Information technology – Open Systems Interconnection – Connection oriented presentation protocol – Part 2: Protocol Implementation Conformance Statement (PICS) Proforma*
- ISO/ISP 14226-1:1996, Industrial automation systems – International Standardized Profile AMM11: MMS General Applications Base Profile – Part 1: Specification of ACSE, Presentation and Session protocols for the use by MMS
- ISO/ISP 14226-2:1996, Industrial automation systems – International Standardized Profile AMM11: MMS General Applications Base Profile – Part 2: Common MMS requirements

The following standards are normative as described in 60870-6-802:

- IEC 60870-5-101:1995, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 101: Companion standard for basic telecontrol tasks*
- IEC 60870-6-503:2002, *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – Section 503: TASE.2 Services and protocol*
- ISO 9506-1:2000, *Industrial automation systems – Manufacturing message specification – Part 1: Service definition*
- ISO 9506-2:2000, *Industrial automation systems – Manufacturing message specification – Part 2: Protocol specification*

3. IEC 61850: Communications Networks and Systems for Power Utility Automation

3.1 Description of Communications Standard

IEC 61850, *Communications Networks and Systems for Power Utility Automation,* specifies both abstract information models (semantic models) and communication services (application layer messaging services) focused on interactions to and between field devices. The semantic models do not need to address security since they are abstract. However, communication services must address security. In IEC 61850, the communication services identify the security requirements, and then state that other standards will provide the security technologies to meet those requirements.

Security for IEC 61850 is provided primarily through IEC 62351 with any necessary updates being made to parts of IEC 61850 to accommodate and reference the security requirements from IEC 62351. It should be noted that currently IEC 62351 is a normative reference in only IEC 61850 Part-90-1, because this part was developed after IEC 62351. Part 90-1 also does address the security of the unique aspects of inter-substation communications.

IEC 61850 is a "living document" and parts will be added that may also cover security. Not all parts of IEC 61850 need to reference IEC 62351, rather only those parts that require cyber security will need to be updated to reflect the normative reference.

It is recommended that during the next review cycle of IEC 61850 that references to IEC 62351 be included where applicable.

Listed below are the parts of IEC 61850 and a general description of what each part contains:

IEC 61850-1: ***Introduction and overview***

- Introduction and overview of IEC 61850

IEC 61850-2: ***Glossary***

- Collection of terms

IEC 61850-3: ***General requirements***

- Quality requirements (reliability, maintainability, system availability, portability, and security)
- Environmental conditions
- Auxiliary services
- Other standards and specifications

IEC 61850-4: ***System and project management***

- Engineering requirements (parameter classification, engineering tools, and documentation)
- System lifecycle (product versions, discontinuation, and support after discontinuation)
- Quality assurance (responsibilities, test equipment, type tests, system tests, FAT and SAT)

IEC 61850-5: ***Communication requirements for functions and device models***

- Basic requirements

- Logical nodes approach
- Logical communication links
- PICOM concept
- Logical Nodes and related PICOMs
- Performance
- Functions
- "Dynamic scenarios" (information flow requirements for different operational conditions)

IEC 61850-6: ***Configuration description language for communication in electrical substations related to intelligent electronic devices (IEDs)***

- Overview on intended system engineering process
- Definition of system and configuration parameter exchange file format based on XML containing:
  - Primary system schematic (single line) description
  - Communication connection description
  - IED capabilities
- Allocation of IED logical node to primary system

IEC 61850-7-1: ***Basic communication structure for substation and feeder equipment – Principles and models***

- Introduction to IEC 61850-7-x
- Communication principles and models

IEC 61850-7-2: ***Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)***

- Description of the ACSI
- Specification of the abstract communication services
- Model of the device database structure

IEC 61850-7-3: ***Basic communication structure for substation and feeder equipment – Common data classes***

- Common data classes and related attributes

IEC 61850-7-4: ***Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes***

- Definitions of logical node classes and data classes; logical node classes are composed of data classes

IEC 61850-8: ***Specific communication service mapping***

- Mapping(s) of services commonly used for communication within the whole substation

IEC 61850-9: ***Specific communication service mapping***

- Mapping(s) of services used for the transmission of sampled analogue values

IEC 61850-10: ***Conformance testing***

- Conformance test procedures
- Quality assurance and testing
- Required documentation
- Device related conformance testing
- Certification of test facilities, requirement and validation of test equipment

IEC 61850-80-1: ***Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104***

- This technical specification is a guideline on how to exchange information from a CDC-based data model (for example IEC 61850) using IEC 60870-5-101 or IEC 60870-5-104 between substation(s) and control center(s). The guideline mostly covers functions needed in a substation gateway device.

IEC 61850-90-1: ***Use of IEC 61850 for the communication between substations***

- Provides a comprehensive overview on the different aspects that need to be considered while using IEC 61850 for information exchange between substations.
- Uniquely in the IEC 61850 series, Part 90-1 does address some security requirements and suggests some solutions. In particular, clause 7 covers considerations on security and dependability issues when using Ethernet networks. The purpose is to highlight the specific issues of Ethernet networks, and provide solutions so substation networks can be engineered to guarantee the security and dependability required by applications for communication between substations.

3.2 Summary of Cyber Security Content

3.2.1 Does the standard address cyber security? If not, should it?

Since IEC 61850 covers both abstract models (semantic models) and the mapping of the abstract models to a communications protocol (application layers), there are two answers to the question of addressing cyber security.

The IEC 61850 abstract model does identify the key cyber security *requirements* that must be met during implementations, but does not attempt to provide the cyber security *solutions*. Security solutions are considered out of scope, as abstract object models should not specify security technologies, since the protocols that these semantic models are mapped to will need to provide the relevant security solutions.

IEC 61850 does specify one mapping – that to the Manufacturers Messaging Specification (MMS). Therefore, security is required from the MMS protocol. IEC 61850 relegates the provision of security solutions of MMS to IEC 62351. To-date, the only part of IEC 61850 that has been recently updated *and* needs to address security is IEC 61850-90-1, which does include a normative reference to IEC 62351-6.

Listed below are the Parts that contain security *requirements* (not solutions):

Part 3 – Page 17 clauses 4.5 and Annex A: Access security Page 31 and 33
Clause 4.5 references IEC 60870-4 clause 3.4 for security.[1] The substation automation system should implement security features that counter, within appropriate user and cost constraints, certain key threats, specifically denial of service and illegitimate use.

Part 5 - Page 49 clause 13.7.7 Command messages with access control and Part 5 - Page 49 clause 14 Requirements for data integrity
The core of 61850 Part 5 is defined in terms of Logical Nodes (LNs) and Pieces of Information for Communications (PICOMs). This Review addresses the need for

[1] This reference is not a normative reference. IEC 60870-4 was not available for review.

security LNs and security PICOMs either explicitly within IEC 61850 or implicitly by normative reference.

Part 6 Ed 2 - Page 69 clause 9.3.3

This clause has a table of authentication types for an IED: None, Password, Weak, Strong, Certificate. This is also represented in the XML scheme on page 131 Annex A.4 IED capabilities and structure and page 184 SCL_Enums.xsd. The part refers to data objects for including security and certificate information in the system configuration language.

Part 7-2 - Page 31 clause 7.3 Access control

This clause describes the access control model and how it provides the capability to restrict the access of a specific client to class instances, class instance attributes, and ACSI services. This security requirement identifies the need to control access on a per-data-element basis, rather than just on an end-device basis.

Part 7-2 - Page 139 clause 17 Control class model

This clause discusses the control of a device with normal and enhanced security. Enhanced security in this context is related to power system reliability requirements for a process called “select-before-operate”. Security in this scenario is the attribute of a confirmed response to a control operation, e.g. did the operation complete successfully or fail? The standard explains the need for confirmation of a control message response, but not the security around the response, such as integrity or confidentiality.

Part 7-4 Ed 2 – Clause 5.7.5 LN: Generic security application Name: GSAL

The GSAL Logical Node provides a means of monitoring (counting) security violations (authorization, access control, service privileges and inactive associations).

IEC 61850-8-1, Clause 10.2.1

This Part specifies the mapping of the abstract models to the MMS protocol. It recognized the need for security of MMS to be addressed, but was released as a standard before IEC 62351 was developed. Therefore, it contains the note: *Security and authentication are future work items. Both are pending the development of a common IEC Technical Committee 57 security mechanism. This mechanism may restrict the visibility of objects within the MMS Environment. These efforts are underway within IEC Technical Committee 57 Working Groups 7 and 15.*

IEC 61850-90-1, Clause 6, 7 and Clause 2

This Part addresses protective relaying interactions between substations with very high speeds, low time latencies, and high availability requirements. It identifies some of the data and communication security considerations and potential solutions when

Ethernet networks are used for these high speed, high availability interactions. This is the only Part updated recently enough *and* with relevant security requirements for it to reference IEC 62351-6.

3.2.2 What aspects of cyber security does the standard address, and how well (correctly) does it do so?

In general, IEC 61850 describes the security *requirements*, but security solutions are left to the mapping of these abstract data models to actual protocols and actual implementations. It is expected, that with some exceptions, the security solutions will be described in the IEC 62351 series.

The applicable NISTIR 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Configuration Management (SG.CM)	SG.CM-5, Access Restrictions for Configuration Change
Identification and Authentication (SG.IA)	sub sections of SG.IA-4, User Identification and Authentication sub sections of SG.IA-5, Device Identification and Authentication
Smart Grid Information System and Communication Protection (SG.SC)	sub sections of SG.SC-5, Denial-Of-Service Protection sub sections of SG.SC-19, Security Roles
Smart Grid Information System and Information Integrity (SG.SI)	sub sections of SG.SI-8, Software and Information Integrity

3.2.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

It is recommended that the next editions of those parts of IEC 61850 that address security requirements should be revised to incorporate IEC 62351 as a normative reference for security.

3.2.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

The next editions of affected parts of IEC 61850 should incorporate IEC 62351 as a normative reference for security. Although this standard, as is, has some security elements, security will be addressed by IEC 62351, which will continue to be expanded to meet new IEC 61850 security requirements.

As new mappings are developed of the abstract IEC 61850 information models to protocols, such as SEP 2.0, DNP3, web services, etc., the security specifications of those mappings will need to address the appropriate security solutions.

3.2.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be reviewed. The focus on these additional reviews should be on ensuring that the security *requirements* identified in the abstract IEC 61850 models are meet by the protocols they are mapped to.

The following standards are normative as described in IEC 61850-1:

- IEC 60870-5-103:1997, *Telecontrol equipment and systems – Part 5-103: Transmission protocols – Companion standard for the informative interface of protection equipment*
- IEC 61850-3: *Communication networks and systems in substations – Part 3: General requirements*
- IEC 61850-5: *Communication networks and systems in substations – Part 5:Communicationre requirements for functions and device models*
- IEC 61850-6: *Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*
- IEC 61850-10: *Communication networks and systems in substations – Part 10: Conformance Testing*

The following standards are informative as described in IEC 61850-2:

- IEC 61850-7-1: *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models*
- IEC 61850-7-2: *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3: *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61850-7-4: *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*
- IEC 61850-9-1: *Communication networks and systems in substations – 3Part 9-1: Specific Communication Service Mapping (SCSM)-Sampled values over serial unidirectional multidrop point to point link*
- IEC 61850-9-2: *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM)-Sampled values over ISO/IEC 8802-*
- IEEE 100,1996, *IEEE Standard Dictionary of Electrical and Electronic Terms*
- IEEE C37.2,1996 *IEEE Standard Electrical Power System Device Function Numbers and Contact Designations*
- IEEE-SA TR 1550,1999: *Utility Communications Architecture (UCA) Version 2.0 – Part 4: UCA Generic Object Models for Substation and Feeder Equipment (GOMSFE)*
- ISO 9001, 2001: *Quality management systems – Requirements*

The following standards are normative as described in IEC 61850-3:

- CISPR 22:1997, *IEEE Standard for Information Technology Equipment. Radio Disturbance Characteristics. Limits and Methods of Measurement*

- IEC 60654-4:1987, *Operating conditions for industrial-process measurement and control equipment. Part 4: Corrosive and erosive influences*
- IEC 60694:1996, *Common specifications for high-voltage switchgear and control gear standards*
- IEC 60870-2-1:1995, *Telecontrol equipment and systems. Part 2: Operating conditions. Section 1: Power supply and electromagnetic compatibility*
- IEC 60870-2-2:1996, *Telecontrol equipment and systems. Part 2: Operating conditions. Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences)*
- IEC 60870-4:1990, *Telecontrol equipment and systems. Part 4: Performance requirements*
- IEC 61000-4-5:1995, *Electromagnetic compatibility (EMC). Part 4: Testing and measurement techniques. Section 5: Surge immunity test*
- IEC 61000-4-6:1996, *Electromagnetic compatibility (EMC). Part 4: Testing and measurement techniques. Section 6: Immunity to conducted disturbances, induced by radio-frequency fields*
- IEC 61000-4-8:1993, *Electromagnetic compatibility (EMC). Part 4: Testing and measurement techniques. Section 8: Power frequency magnetic field immunity test*
- IEC 61000-4-10:1993, *Electromagnetic compatibility (EMC). Part 4: Testing and measurement techniques. Section 10: Damped oscillatory magnetic field immunity test*
- IEC 61000-4-12:1995, *Electromagnetic compatibility (EMC). Part 4: Testing and measurement techniques. Section 12: Oscillatory waves immunity test*
- IEC 61000-4-16:1998, *Electromagnetic compatibility (EMC). Part 4-16: Testing and measurement techniques. Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz*
- IEC TS 61000-6-5:2001, *Electromagnetic compatibility (EMC). Part 6-5: Generic standards Immunity for power station and substation environments*
- CISPR 22:1997, *IEEE Standard for Information Technology Equipment. Radio Disturbance Characteristics. Limits and Methods of Measurement*
- IEEE C37.90.2:1995, *IEEE Standard for Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers*

The following standards are informative as described in IEC 61850-3:

- IEC 61000-4-3:1995, *Electromagnetic compatibility (EMC). Part 4: Testing and measurement techniques. Section 3: Radiated, radio-frequency, electromagnetic field immunity test*
- IEC 61000-4-4:1995, *Electromagnetic compatibility (EMC). Part 4: Testing and measurement techniques. Section 4: Electrical fast transient/burst immunity test.* Basic EMC Publication

The following standards are normative as described in IEC 61850-4:

- IEC 60848:1988, *Preparation of function charts for control systems*
- IEC 61082 (all parts), *Preparation of documents used in the electro technology*
- IEC 61175:1993, *Designations for signals and connections*
- IEC 61346 (all parts), *Industrial systems, installations and equipment and industrial products. Structuring principles and reference designations*
- ISO 9001:1994, *Quality systems. Model for quality assurance in design, development, production, installation and servicing*

The following standards are normative as described in IEC 61850-5:

- IEC 60044-8, *Instrument transformers – Part 8: Electronic current transformers*
- IEC 60870-4, *Telecontrol equipment and systems – Part 4: Performance requirements*
- IEC 61346 (all parts), *Industrial systems, installations and equipment and industrial products – Structuring principles and reference designations*
- IEC 61850-2, *Communication networks and system in substations – Part 2: Glossary* 3
- IEC 62053-22, *Electricity metering equipment (a.c.) – Particular Requirements – Part 22: Static meters for active energy (classes 0,2 S and 0,5 S)*
- IEEE Std C37.2:1996, *IEEE Standard Electrical Power System Device Function Numbers and Contact Designations*

The following standards are normative as described in IEC 61850-6 Ed 2:

- IEC 61850-2, *Communication networks and systems in substations – Part 2: Glossary*
- IEC 61850-5, *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models*
- IEC 61850-7-1, *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models*
- IEC 61850-7-2, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61850-7-4, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*
- IEC 61850-8-1, *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*
- IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*
- IEC 81346-1, *Industrial systems, installations and equipment and industrial products – Structuring principles and reference designations – Part 1: Basic rules*
- ISO/IEC 8859-1, *Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*
- RFC 1952, *GZIP file format specification version 4.3*
- RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*
- *Extensible Markup Language (XML) 1.0*, W3C
- *XML Schema Part 1: Structures,* W3C
- *XML Schema Part 2: Datatypes*, W3C

The following standards are normative as described in IEC 61850-7-1:

- IEC 61850-2, *Communication networks and systems in substations – Part 2: Glossary* 3
- IEC 61850-5, *Communication networks and systems in substations – Part 5: Communication requirements for functions and devices models* 3

- IEC 61850-7-2, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61850-7-4, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*
- ISO/IEC 8802-3:2000, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements –Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*
- ISO/IEC 8825 (all parts), *Information technology – ASN.1 encoding rules*
- ISO 9506-1:2003, *Industrial automation systems – Manufacturing Message Specification – Part 1: Service definition*
- ISO 9506-2:2003, *Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification*

The following standards are normative as described in IEC 61850-7-2:

- IEC 61850-2, *Communication networks and systems in substations – Part 2: Glossary*
- IEC 61850-5, *Communication networks and systems in substations – Part 5: Communication requirements for functions and devices models*
- IEC 61850-7-1, *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models*
- IEC 61850-7-3, *Communication networks and systems in substations – Part 7-3*: *Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61850-7-4, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*
- IEC 61850-8-1: *Communication networks and systems in substations – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3*

The following standards are normative as described in IEC 61850-7-3:

- IEC 61850-2, *Communication networks and systems in substations – Part 2: Glossary* 3
- IEC 61850-7-1, *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models*
- IEC 61850-7-2, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-4, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*
- ISO 1000, *SI units and recommendations for the use of their multiples and of certain other units*

The following standards are normative as described in IEC 61850-7-4:

- IEC 60255-24, *Electrical relays – Part 24: Common format for transient data exchange (COMTRADE) for power systems*
- IEC 61000-4-7, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 7: General guide on harmonics and interharmonics measurements and instrumentation for power supply systems and equipment connected thereto*
- IEC 61850-2, *Communication networks and system in substations – Part 2: Glossary*
- IEC 61850-5, *Communication networks and systems in substations – Part 5: Communication requirements for functions and devices models*
- IEC 61850-7-1, *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models*
- IEC 61850-7-2, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEEE 519:1992, *IEEE Recommended Practises and Requirements for Harmonic Control in Electrical Power Systems*
- IEEE 1459:2000, *IEEE Trial Use Standard Definitions for the Measurement of Electric Power Quantities Under Sinusoidal, Nonsinusoidal, Balanced or Unbalanced Conditions*
- IEEE C37.2:1996, *Electrical Power System Device Function Numbers and Contact Designation*

The following standards are normative as described in IEC 61850-7-410:

- IEC 61850-2, Communication networks and systems in substations – Part 2: Glossary
- *IEC 61850-5, Communication networks and systems in substations – Part 5: Communication requirements for functions and device models*
- *IEC 61850-6, Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*
- *IEC 61850-7-2:2003, Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication services interface (ACSI)*
- *IEC 61850-7-3:2003, Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- *EC 61850-7-4:2003, Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes*

The following standards are normative as described in IEC 61850-7-420:

- IEC 61850-7-2:2003, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substations and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3:2003, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substations and feeder equipment – Common data classes*

- IEC 61850-7-4:2003*, Communication networks and systems in substations – Part 7-4: Basic communication structure for substations and feeder equipment – Compatible logical node classes and data classes*
- IEC 61850-7-410, *Communication networks and systems for power utility automation – Part 7-410: Hydroelectric power plants – Communication for monitoring and control*
- ISO 4217, *Codes for the representation of currencies and funds*

The following standards are normative as described in IEC 61850-8-1:

- IEC 60874-10-1:1997*, Connectors for optical fibres and cables – Part 10-1: Detail specification for fibre optic connector type BFOC/2,5 terminated to multimode fibre type A1*
- IEC 60874-10-2:1997, *Connectors for optical fibres and cables – Part 10-2: Detail specification for fibre optic connector type BFOC/2,5 terminated to single-mode fibre type B1*
- IEC 60874-10-3:1997, Connectors *for optical fibres and cables – Part 10-3: Detail specification for fibre optic connector type BFOC/2,5 for single and multimode fibre*
- IEC 61850-2, *Communication networks and systems in substations – Part 2: Glossary*
- IEC 61850-5, *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models*
- IEC 61850-7-1, *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Part 7-1: Principles and models*
- IEC 61850-7-2, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61850-7-4, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*
- IEC 61850-9-1, *Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link*
- IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*
- ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*
- ISO/IEC 7498-3:1997, *Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing*
- ISO/IEC 8072:1996, *Information technology – Open systems interconnection – Transport service*
- ISO/IEC 8073:1997, *Information technology – Open Systems Interconnection – Protocol for providing the connection-mode transport service definition*
- ISO/IEC 8326:1996, *Information processing system – Open Systems Interconnection – Session service definition*
- ISO/IEC 8327-1:1997, Information *technology – Open Systems Interconnection – Connection- oriented session protocols: Protocol specification*
- ISO/IEC 8348:2002, *Information technology – Open Systems Interconnection – Network service definition*

- ISO/IEC 8473-1:1998, *Information technology – Protocol for providing the connectionless-mode network service: Protocol specification*
- ISO/IEC 8473-2:1996, *Information technology – Protocol for providing the connectionless- mode network service – Part 2: Provision of the underlying service by an ISO/IEC 8802 subnetwork*
- ISO/IEC 8602:1995, *Information technology – Protocol for providing the OSI connectionless- mode transport service*
- ISO/IEC 8649:1996, *Information technology – Open Systems Interconnection – Service definition for the Associated Control Service Element*
- ISO/IEC 8650-1:1996, *Information technology – Open Systems Interconnection – Connection- oriented protocol for the Association Control Service Element: Protocol specification*
- ISO/IEC 8802-2:1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control*
- ISO/IEC 8802-3:2001, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*
- ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – Presentation service definition*
- ISO/IEC 8823-1:1994, *Information technology – Open Systems Interconnection – Connection- oriented presentation protocol: Protocol specification*
- ISO/IEC 8824-1:1999, *Information technology – Abstract Syntax Notation One (ASN. 1): Specification of basic notation Amendment 1 (2000), Amendment 2 (2000)*
- ISO/IEC 8825-1:2000, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*
- ISO/IEC 8877:1992, *Information technology – Telecommunications and information exchange between systems – Interface connector and contact assignments for ISDN Basic Access Interface located at reference points S and T*
- ISO/IEC 9542:1988, *Information processing systems – Telecommunications and information exchange between systems – End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*
- ISO/IEC 9548-1:1996, *Information technology – Open Systems Interconnection – Connection- less Session protocol: Protocol specification*
- ISO/IEC 9576-1:1995, *Information technology – Open Systems Interconnection – Connection- less Presentation protocol: Protocol specification*
- ISO/IEC 10035-1:1995, *Information technology – Open Systems Interconnection – Connection- less protocol for the Association Control Service Element: Protocol specification Amendment 1 (1998)*
- ISO/IEC ISP 10608-1:1992, *Information technology – International Standardized Profile TAnnnn – Connection-mode Transport Service over Connectionless-mode Network Service – Part 1: General overview and subnetwork-independent requirements*
- ISO/IEC ISP 10608-2:1992, *Information technology – International Standardized Profile TAnnnn – Connection-mode Transport Service over Connectionless-mode Network Service – Part 2: TA51 profile including subnetwork-dependent requirements for CSMA/CD Local Area Networks (LANs)*

- ISO/IEC ISP 11188-1:1995, *Information technology – International Standardized Profile – Common upper layer requirements – Part 1: Basic connection oriented requirements*
- ISO/IEC ISP 11188-3:1996, *Information technology – International Standardized Profile – Common upper layer requirements – Part 3: Minimal OSI upper layer facilities*
- ISO 9506-1:2003, *Industrial automation systems – Manufacturing Message Specification – Part 1: Service definition ISO 9506-2:2003, Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification*
- ISO/ISP 14226-1:1996, *Industrial automation systems – International Standardized Profile AMM11: MMS General Applications Base Profile – Part 1: Specification of ACSE, Presentation and Session protocols for use by MMS*
- ISO/ISP 14226-2:1996, *Industrial automation systems – International Standardized Profile AMM11: MMS General Applications Base Profile – Part 2: Common MMS requirements*
- *ISO/ISP 14226-3:1996, Industrial automation systems – International Standardized Profile AMM11: MMS General Applications Base Profile – Part 3: Specific MMS requirements*
- IEEE C37.111:1999, *IEEE Standard for Common Format for Transient Data Exchange (COMTRADE) for Power Systems*
- IEEE 754:1985, *IEEE Standard for Binary Floating-Point Arithmetic*
- IEEE 802.1Q:1998, *IEEE Standards for Local and Metropolitan Networks: Virtual Bridged Local Area Networks*
- RFC 542, *File Transfer Protocol for the ARPA Network*, IETF, available at http://www.ietf.org
- RFC 768, *U ser Datagram Protocol*, IETF, available at http://www.ietf.org
- RFC 791, *Internet Protocol – DARPA Internet Program Protocol Specification*, IETF, available at http://www.ietf.org
- RFC 792, Internet *Control Message Protocol – DARPA Internet Program Protocol Specification*, IETF, available at http://www.ietf.org
- RFC 793, *Transmission Control Procedure – DARPA Internet Program Protocol Specification*, IETF, available at http://www.ietf.org
- RFC 826, *An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, IETF, available at http://www.ietf.org
- RFC 894, *A Standard for the Transmission of IP datagrams over Ethernet Networks*, IETF, available at http://www.ietf.org
- RFC 919, *Broadcasting Internet Datagrams*, IETF, available at http://www.ietf.org
- RFC 922, *Broadcasting Internet Datagrams in the presence of subnets*, IETF, available at http://www.ietf.org
- RFC 950, *Internet Standard Subnetting Procedure*, IETF, available at http://www.ietf.org
- RFC 959, *File Transfer Protocol (FTP)*, IETF, available at http://www.ietf.org
- RFC 1006, *ISO transport services on top of TCP: Version 3*, IETF, available at http://www.ietf.org
- RFC 1112, *Host Extensions for IP Multicasting*, IETF, available at http://www.ietf.org
- RFC 1122, *Requirements for Internet Hosts – Communication Layers*, IETF, available at http://www.ietf.org
- RFC 1123, *Requirements for Internet Hosts – Application and Support*, IETF, available at http://www.ietf.org
- RFC 2030, *Simple Network Time Protocol (SNTP) Version 4*, IETF, available at http://www.ietf.org

The following standards are normative as described in IEC 61850-9-1:

- IEC 60044-7: *Instrument Transformers – Part 7: Electronic voltage transformers*
- IEC 60044-8: *Instrument Transformers – Part 8: Electronic current transformers*
- IEC 60874-10-1:1997, *Connectors for optical fibers and cables – Part 10-1: Detail specification for fiber optic connector type BFOC/2,5 terminated to multimode fiber type A1*
- IEC 61850-7-2: *Communication networks and systems in substations – Part 7-2: Basic communication -structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3: *Communication networks and systems in substations – Part 7-3: Basic Communication structure for substation and feeder equipment – Common data classes*
- ISO/IEC 8802-3: *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3:Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*
- ISO/IEC 8825-1: *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*
- IEEE 802.1Q-1998: *IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*
- IEEE 802.3: *Information Technology – Telecommunication and Information Exchange Between Systems – LAN/MAN – Specific Requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

The following standards are normative as described in IEC 61850-9-2:

- IEC 60874-10-1, *Connectors for optical fibers and cables – Part 10-1: Detail specification for fiber optic connector type BFOC/2,5 terminated to multimode fiber type A1*
- IEC 60874-10-2, *Connectors for optical fibers and cables – Part 10-2: Detail specification for fiber optic connector type BFOC/2,5 terminated to single-mode fiber type B1*
- IEC 60874-10-3, *Connectors for optical fibers and cables – Part 10-3: Detail specification for fiber optic adaptor type BFOC/2,5 for single and multimode fibre*
- IEC 61850-7-2, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (*ACSI *)*
- IEC 61850-7-3, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61850-8-1, *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (*SCSM*) – Mappings to* MMS *(ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*
- IEC 61850-9-1, *Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (*SCSM*) – Sampled values over serial unidirectional multidrop point to point link*
- ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

- ISO/IEC 8326:1996, *Information processing systems – Open Systems Interconnection – Session service definition*
- ISO/IEC 8327-1:1997, *Information technology – Open Systems Interconnection – Connection oriented session protocols: Protocol specification*
- ISO/IEC 8649:1996, *Information technology – Open Systems Interconnection – Service definition for the Associated Control Service Element*
- ISO/IEC 8650-1:1996, *Information technology – Open Systems Interconnection – Connection oriented protocol for the Association Control Service Element: Protocol specification*
- ISO/IEC 8802-3:2001, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*
- ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – Presentation service definition*
- ISO/IEC 8823-1:1994, *Information technology – Open Systems Interconnection – Connection oriented presentation protocol: Protocol specification*
- ISO/IEC 8824-1:1999, *Information technology – Abstract Syntax Notation One (ASN. 1): Specification of basic notation* Amendment 1 (2000) Amendment 2 (2000)
- ISO/IEC 8825-1, *Information technology –* ASN.1 *encoding rules: Specification of Basic Encoding Rules (*BER*), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*
- ISO 9506-1:2003, *Industrial automation systems – Manufacturing Message Specification – Part 1: Service definition*
- ISO 9506-2:2003, *Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification*
- IEEE 754:1985, *IEEE Standard for Binary Floating-Point Arithmetic*
- IEEE 802.1Q:1998*, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*
- RFC 791, *Internet Protocol; IETF, available at <http://www.ietf.org>*
- RFC 792, *Internet Control Message Protocol; IETF, available at <http://www.ietf.org>*
- RFC 793, *Transmission Control Procedure; IETF, available at <http://www.ietf.org>*
- RFC 826, *An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware;*
- RFC 894, *A Standard for the Transmission of IP datagrams over Ethernet Networks;*
- RFC 919, *Broadcasting Internet Datagrams;*
- RFC 1006 *ISO transport services on top of TCP: Version 3;*
- RFC 1112, *Host Extensions for IP Multicasting;*

The following standards are informative as described in IEC 61850-9-2:

- IEC 61850-7-1, *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Part 7-1: Principles and models*
- IEC 61850-7-4, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*

The following standards are normative as described in IEC 61850-80-1:

- IEC 60870-5-3, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 3: General structure of application data*
- IEC 60870-5-4:1993, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 4: Definition and coding of application information elements*
- IEC 60870-5-5:1995, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 5: Basic application functions*
- IEC 60870-5-101:2003, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*
- IEC 60870-5-104:2006, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*
- IEC 61850 (all parts), *Communication networks and systems in substations*
- IEC 61850-6, *Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*
- IEC 61850-7-2:2003, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)*
- IEC 61850-7-3*, Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61850-8-1, *Communication networks and systems in substations – Part 8-1: Specific Communications Service Mapping (SCSM) – Mapping to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*
- Document 57/963/INF: *IEC 61850 – Technical issues* (see www.tissue.iec61850.com)
- IEC 61400-25-2, *Wind turbines – Part 25-2: Communications for monitoring and control of wind power plants – Information models*
- IEEE 754:2008*, IEEE Standard for Binary Floating-Point Arithmetic*
- RFC 2200*, Internet Official Protocol Standards, Request for Comments 2200 (June 1997)*

The following standards are normative as described in IEC 61850-90-1:

- IEC 60044 (all parts), *Instrument transformers*
- IEC 60834-1:1999, *Teleprotection equipment of power systems – Performance and testing – Part 1: Command systems*
- IEC 60834-2:1993*, Performance and testing of teleprotection equipment of power systems – Part 2: Analogue comparison systems*
- IEC 60870-4, *Telecontrol equipment and systems – Part 4: performance requirements*
- IEC/TS 61850-2, *Communication networks and systems in substations – Part 2: Glossary*
- IEC 61850 (all parts), *Communication networks and systems for power utility automation*
- IEC 61850-3, *Communication networks and systems in substations – Part 3: General requirements*
- IEC 61850-5:2003, *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models*
- IEC 61850-6:2009, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*
- IEC 61850-7-2:2010, C*ommunication networks and systems for power utility automation – Part 7-2: Basic communication structure – Abstract communication service interface (ACSI)*

- IEC 61850-7-4:2010, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*
- IEC 61850-8-1,___ *Communication networks and systems for power utility automation – Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*2)
- IEC 61850-9-2,___ *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*2)
- IEC 62053-22, *Electricity metering equipment (a.c.) – Particular requirements – Part 22: Static meters for active energy (classes 0,2 S and 0,5 S)*
- IEC/TS 62351-6, *Power systems management and associated information exchange – Data and communication security – Part 6: Security for IEC 61850*
- IEC 62439, *High availability automation networks*
- ANSI/IEEE 1588, *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems / revision of ANSI/IEEE 1588-2002 / Approved 2008-09-10*
- IEEE 802.1Q, *Local and metropolitan area networks – Virtual bridged local area networks*

4. IEC 61968: CIM and Messaging Interfaces for Distribution Management

4.1 Description of Communications Standard

IEC 61968 defines abstract information models and abstract messaging interfaces for the major elements of an interface architecture for Distribution Management Systems (DMS). No methods or technologies for mapping these abstract models to protocols are included, because they are considered outside of the scope of this standard. The standard is considered to be entirely abstract and implementation independent. Security is not considered to be in scope of the standard.

This standard is focused on the development of an abstract Common Information Model (CIM) and the definition of abstract messages based on the CIM. Part 1 of IEC 61968 identifies and establishes the non-security-related requirements for standard interfaces based on an Interface Reference Model (IRM). Security requirements are addressed very generally[2] and these generalities, which are currently in the form of "shall statements," are being removed in subsequent editions.

Other parts of this standard are based on each interface identified in the IRM. They provide for interoperability among different computer systems, platforms, and languages. Additional parts reflect new interfaces identified since the original IRM was developed, including MultiSpeak models.

The parts of IEC 61968, Application Integration at Electric Utilities-System Interfaces for Distribution Management, as listed as follows:

61968-01: Interface Architecture and General Requirements
61968-01-1: Enterprise Service Bus Implementation Profile
61968-01-2: Web Services
61968-02: Glossary
61968-03: Network Operations
61968-04: Records & Asset Management
61968-05: Operational Planning and Optimization
61968-06: Maintenance and Construction
61968-07: Network Extension Planning
61968-08: Customer Support
61968-09: Meter Reading and Control
61968-11: Common Information Model for DMS
61968-12: Compliance and Interoperability Testing
61968-13: Common Distribution Power System Model
61968-14: MultiSpeak Model

4.2 Summary of Cyber Security Content

4.2.1 Does the standard address cyber security? If not, should it?

No, this standard focuses on the development of abstract information models, does not include any protocols, and assumes that any mapping of the abstract models to actual

[2] IEC 61968-1, clause 8.1: *An IEC 61968 compliant system shall implement security requirements as determined by the utilities security policy*.

protocols or application components will utilize appropriate security. Methods and technologies used to implement functionality conforming to this CIM standard, including security, are considered outside of the scope of this standard; only the abstract models are specified in the IEC 61968 series.

4.2.2 What aspects of cyber security does the standard address and how well (correctly) does it do so?

This standard recognizes that security is needed by the protocols or application components. It provides guidance in Part 1, Chapter 8 for the application components forming an IEC 61968 series compliant system using "shall" statements such as "*The agreed utility policy shall determine which security and authentication features are required*." However, that statement is currently being removed in the next edition of Part 1. All remaining discussion of security will also be updated to use the term "should" rather than "shall."

4.2.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

The IEC 61968 only acknowledges that security is required for any implementation that uses the CIM. ***However, it is recommended that security guidelines be developed that cover implementations of IEC 61968. In addition to general guidance, these security guidelines should reference appropriate security standards.***

4.2.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

There are planned updates for the standard but they are not for addressing gaps in security. Below is a list of planned updates: [3]

61968-01: Update planned for 2010
61968-01-1: CDV[4] Planned for 2010
61968-01-2: CDV planned for 2010
61968-03: Under Development - Planned for 2011
61968-04: Under Development - Planned for 2011
61968-05: Under development
61968-06: Under Development – CDV planned for 2011
61968-08: Under Development - CDV planned for 2011
61968-09: Under Development - Planned for 2011
61968-13: Under Development - Planned for 2011
61968-14-1: Proposed - Drafting will begin pending interoperability test
61968-14-2: Proposed - Drafting will begin pending interoperability test

Parts that are not listed do not have a scheduled update planned.

[3] Status obtained from the SGIP IKB standard information web site.
[4] Committee Draft for Vote

4.2.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed.

The following standards are normative as described in 61968-3:

- IEC 61850-7-4:2003, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes*
- IEC 61968-1, *System interfaces for distribution management – Part 1: Interface architecture and general requirements*

The following standards are normative as described in 61968-4:

- IEC 61968-1*, Application integration at electric utilities – System interfaces for distribution management – Part 1: Interface architecture and general requirements*
- IEC 61968-3, *Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations*

The following standards are normative as described in 61968-9:

- IEC 60050-300, *International Electrotechnical Vocabulary – Electrical and electronic measurements and measuring instruments – Part 311: General terms relating to measurements – Part 312: General terms relating to electrical measurements – Part 313: Types of electrical measuring instruments – Part 314: Specific terms according to the type of instrument*
- IEC 61968-1*, Application integration at electric utilities – System interfaces for distribution management – Part 1: Interface architecture and general requirements*
- IEC 61968-2*, Application integration at electric utilities – System interfaces for distribution management – Part 2: Glossary*
- IEC 61968-3, *Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations*
- IEC 61970-301, *Energy management system application program interface (EMS-API) – Part 301: Common information model (CIM) base*
- IEC 62051-1, *Electricity metering – Data exchange for meter reading, tariff and load control –Glossary of terms – Part 1: Terms related to data exchange with metering equipment using DLMS/COSEM*
- IEC 62055-31, *Electricity metering – Payment systems – Part 31: Particular requirements –Static payment meters for active energy (classes 1 and 2)*
- IEC 62056 (all parts), *Electricity metering – Data exchange for meter reading, tariff and load control*
- ISO 4217, *Codes for the representation of currencies and funds*
- ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*
- ANSI C12.19, *Utility Industry End Device Data Tables*

The following standards are normative as described in 61968-13:

- IEC 61968-1*, Application integration at electric utilities – System interfaces for distribution management – Part 1: Interface architecture and general requirements*

- IEC 61968-3, *Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations*
- *IEC 61968-4,* Application integration at electric utilities – System interfaces for distribution management – Part 4: Interfaces for records and asset management
- *IEC 61970-301*, Energy management system application program interface (EMS-API) – Part 301: Common Information Model (CIM) base
- IEC 61970-501, *Energy management system application program interface (EMS-API) – Part 501: Common Information Model Resource Description Framework (CIM RDF) schema*

5. IEC 61970: Common Information Model (CIM) for Wires Models

5.1 Description of Communications Standard

The IEC 61970 series is strictly an abstract model of power system configurations and organizations. Unlike IEC 61968, IEC 61970 does not include any messaging structures, which is assumed to be provided by mapping to other standards.

Part 1 of the IEC 61970 series describes typical integration scenarios where these standards are to be applied and the types of applications to be integrated. A reference model is defined to provide a framework for the application of the other parts of the Energy Management System Application Programming Interface (EMS-API) standards. This reference model is based on a component architecture that places the focus of the standards on component interfaces for information exchange between applications in a control center environment. While the primary objective of the EMS-API is to support the integration of applications within the control center, the reference model is also applicable to information exchanges between control center applications and systems external to the control center environment, such as other control centers, independent system operators (ISOs), regional transmission operators (RTOs), and distribution systems.

This standard describes the role of the other parts of the standard, including the CIM in the IEC 61970-3XX series, the Component Interface Specifications (CIS) in the IEC 61970-4XX series, and Technology Mappings in the IEC 61970-5XX series.

Although Part 1 mentions the need for security services, it does not specifically identify which services or for what purposes, since this standard focuses only on abstract object models, and not on protocols. Some security references are for the obsolete Corba technologies, and will be deprecated in the next edition.

Listed below are the parts of IEC 61970, Energy Management System Application Program Interface (EMS-API):

61970-1: Guidelines and general requirements
61970-2: Glossary
61970-301: Common Information Model (CIM) base
61970-302: Common information model (CIM) financial, energy scheduling and reservations
61970-401: Component interface specification (CIS) framework
61970-402: Component interface specification (CIS) – Common services
61970-403: Component interface specification (CIS) – Request and Replay
61970-404: Component interface specification (CIS) – High Speed Data Access
61970-405: Component interface specification (CIS) – Generic Eventing and Subscription
61970-407: Component interface specification (CIS) – Historical Data Access
61970-453: Exchange of Graphics Schematics Definitions (Common Graphics Exchange)
61970-501: Common Information Model (CIM) XML Codification for Programmable Reference and Model Data Exchange

5.2 Summary of Cyber Security Content

5.2.1 Does the standard address cyber security? If not, should it?

No, this standard does not address cyber security, rather, it focuses on the development of abstract information models (called CIMs). It does not include any protocols, and assumes that any mapping of the abstract models to actual protocols will utilize appropriate security. The standard acknowledges that security is required for any implementation that uses the CIM, but does not identify security technologies or procedures. Methods and technologies used to implement functionality conforming to these CIM standards are considered outside of the scope of these standards; only the abstract models are specified in the IEC 61970 series.

5.2.2 What aspects of cyber security does the standard address, and how well (correctly) does it do so?

This standard does not (and does not need to) address security but rather focuses on the development of the abstract models of CIM.

5.2.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

This standard does not need to address security. ***However, it is recommended that security guidelines be developed that cover implementations of IEC 61970. In addition to general guidance, these security guidelines should reference appropriate security standards.***

5.2.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

There are planned updates for the standard but they are not for addressing gaps in security. Below is a list of planned updates: [5]

61970-403: Will be retired
61970-404: Will be retired
61970-405: Will be retired
61970-407: Will be retired
61970-450: CIS Information Exchange Model Specification Guide Working draft – currently on hold
61970-454: Naming Service, Working draft
61970-455: Model Population Interfaces, On hold
61970-552-4: CML XML Model Exchange Format, Working draft

Parts that are not listed do not have a scheduled update planned.

[5] Status obtained from the SGIP IKB standard information web site.

5.2.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed.

The following standards are normative as described in 61970-1:

- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- IEC 61970-301, *Energy management system application program interface (EMS-API) – Part 301: Common Information Model (CIM) base*

The following standards are normative as described in 61970-2:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*

The following standards are normative as described in 61970-301:

- IEC 60870 (all parts), *Telecontrol equipment and systems*
- IEC 61850 (all parts), *Communication networks and systems in substations*
- IEC 61850-7-3, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*
- IEC 61968 (all parts), *Application integration at electric utilities – System interfaces for distribution management*
- ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*
- IEEE 754-1985, *Standard for Binary Floating-Point Arithmetic*

The following standards are normative as described in 61970-401:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*
- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- *Utility Management System (UMS) Data Access Facility (DAF)*, OMG Adopted Specification,
  Version 2.0, formal/02-11-08, November 2002 (Referred to herein as 'OMG reference 1')
- *Data Acquisition from Industrial Systems Specification (DAIS),* OMG Adopted Specification,
  Version 1.0, formal/02-11-07, November 2002 (Referred to herein as 'OMG reference 2')
- *Historical Data Acquisition from Industrial Systems Specification (HDAIS),* OMG Adopted
  Specification, dtc/03-02-01, February 2003 (Referred to herein as 'OMG reference 3')
- *OPC Data Access Custom Interface Specification,* Version 2.05, OPC file: opcda205_cust.doc, OPC Foundation, December 17, 2000 (Referred to herein as 'OPC reference 1')
- *OPC Alarms and Events Custom Interface Specification,* Version 1.02, OPC file: opcae102_cust.doc, OPC Foundation, November 2, 1999 (Referred to herein as 'OPC reference 2')

- *OPC Historical Data Access Custom Interface Standard,* Version 1.1, OPC file: opc_hist_cust.doc, OPC Foundation, January 26, 2001 (Referred to herein as 'OPC reference 3')

The following standards are normative as described in 61970-402:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*
- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- IEC 61970-401, *Energy management system application program interface (EMS-API) – Part 401: Component interface specification (CIS) framework*
- IEC 61970-403, *Energy management system application program interface (EMS-API) – Part 403: Component Interface Specification (CIS) – Generic data access*
- IEC 61970-404, *Energy management system application program interface (EMS-API) – Part 404: High Speed Data Access (HSDA)*
- IEC 61970-405, *Energy management system application program interface (EMS-API) – Part 405: Generic Eventing and Subscription (GES)*
- IEC 61970-407, *Energy management system application program interface (EMS-API) – Part 407: Time Series Data Access (TSDA)*
- OMG, *Utility Management System Data Access Facility,* document formal/2002-11-08

The following standards are normative as described in 61970-403:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*
- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- IEC 61970-401, *Energy management system application program interface (EMS-API) – Part 401: Component interface specification (CIS) framework*
- IEC 61970-402, *Energy management system application program interface (EMS-API) – Part 402: Component interface specification (CIS) – Common services*
- OMG, *Utility Management System Data Access Facility,* document formal/2002-11-08

The following standards are normative as described in 61970-404:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*
- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- IEC 61970-301:2005, *Energy management system application program interface (EMS-API) –Part 301: Common Information Model (CIM) base*
- IEC 61970-401, *Energy management system application program interface (EMS-API) – Part 401: Component Interface Specification (CIS) Framework*
- IEC 61970-402, *Energy management system application program interface (EMS-API) – Part 402: Component Interface Specification (CIS) – Common Services*
- *Data Acquisition from Industrial Systems section Data Access (DAIS DA),* OMG Adopted Specification Version 1.1, formal/05-06-01 June 2005 (Referred herein as 'OMG DAIS DA')

- *OPC Data Access Custom Interface Specification,* Version 2.05, OPC file: opcda205_cust.doc, OPC Foundation, December 17, 2000 (Referred to herein as 'OPC DA')

The following standards are informative as described in 61970-404:

- *Utility Management System (UMS) Data Access Facility (DAF),* OMG Adopted Specification, Version 2.0.1, formal/05-06-03, July 2005 (Referred to herein as 'OMG DAF')

The following standards are normative as described in 61970-405:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*
- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- IEC 61970-301:2005, *Energy management system application program interface (EMS-API) –Part 301: Common Information Model (CIM) base*
- IEC 61970-401, *Energy management system application program interface (EMS-API) – Part 401: Component Interface Specification (CIS) Framework*
- IEC 61970-402, *Energy management system application program interface (EMS-API) – Part 402: Component Interface Specification (CIS) – Common Services*
- *Data Acquisition from Industrial Systems section Alarms and Events (DAIS A&E),* OMG Adopted Specification Version1.1, formal/2005-06-01 June 2005 (Referred herein as 'OMG DAIS A&E')
- *OPC Alarms and Events Specification,* Version 1.10, OPC Foundation, October 2002 Referred to herein as 'OPC A&E')

The following standards are informative as described in 61970-405:

- *Utility Management System (UMS) Data Access Facility (DAF),* OMG Adopted Specification, Version 2.0.1, formal/05-06-03, July 2005 (Referred to herein as 'OMG DAF')

The following standards are normative as described in 61970-407:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*
- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- IEC 61970-301:2005, *Energy management system application program interface (EMS-API) –Part 301: Common Information Model (CIM) base*
- IEC 61970-401, *Energy management system application program interface (EMS-API) – Part 401: Component Interface Specification (CIS) Framework*
- IEC 61970-402, *Energy management system application program interface (EMS-API) – Part 402: Component Interface Specification (CIS) – Common Services*
- *Historical Data Access from Industrial Systems (HDAIS),* OMG Adopted Specification Version 1.0, dtc/2003-02-01 November 2003 (Referred herein as 'OMG HDAIS')
- *Data Acquisition from Industrial Systems (DAIS),* OMG Adopted Specification Version 1.0, formal/2002-11-07 November 2002 (Referred herein as 'OMG DAIS')

- *OPC Historical Data Access Custom Interface Specification,* Version 1.20, OPC Foundation, December 2003 (Referred to herein as 'OPC HDA')

The following standards are informative as described in 61970-407:

- *Utility Management System (UMS) Data Access Facility (DAF),* OMG Adopted Specification, Version 2.0.1, formal/05-06-03, July 2005 (Referred to herein as 'OMG DAF')

The following standards are normative as described in 61970-453:

- IEC 61970 (all parts), *Energy Management System Application Program Interface (EMS-API)*
- IEC 61970-301, *Energy management system application program interface (EMS-API) – Part 301: Common information model (CIM) base*
- IEC 61970-402, *Energy management system application program interface (EMS-API) – Part 402: Common services*
- IEC 61970-501*, Energy management system application program interface (EMS-API) – Part 501: Common Information Model Resource Description Framework (CIM RDF) schema*

The following standards are normative as described in 61970-501:

- IEC 61970-2, *Energy management system application program interface (EMS-API) – Part 2: Glossary*
- IEC 61970-301:2005, *Energy management system application program interface (EMS-API) –Part 301: Common Information Model (CIM) base*

The following standards are informative as described in 61970-501:

- IEC 61970-1, *Energy Management System Application Program Interface (EMS-API) – Part 1:Guidelines and general requirements*
- IEC 60050 series: *International Electrotechnical Vocabulary*

6. IEC 62351: Power Systems Management and Associated Information Exchange – Data and Communications Security

6.1 Description of Communication Standard

IEC 62351, Parts 1-8, *Information Security for Power System Control Operations,* are explicitly security standards for:

- Power system management,
- Power system information exchange,
- Communications network and system security issues,
- TCP/IP and MMS profiles,
- Security for ICCP, and
- Substation automation and protection.

This series has been developed to handle the cyber security of the communication protocols defined by IEC TC 57 series of protocols including:

- IEC 60870-5 series,
- IEC 60870-6 series,
- IEC 61850 series,
- IEC 61968 series, and
- IEC 61970 series.

An overview of each of part of IEC 62351 (1-7) is included below. IEC 62351 Part 8 is currently in draft form and will not be assessed until it is finalized.

6.1.1 IEC 62351-1: Introduction to Security Issues

Part 1 provides an introduction to the remaining parts of the standard by introducing readers to various aspects of information security applied to power system operations. This part includes scope, general information, background, and a high-level overview of the remaining parts of the series.

6.1.2 IEC 62351-2: Glossary of Terms

Part 2 of the IEC 62351 series covers the key terms used in the series, including references to original definitions of cyber security terms and communications terms. The glossary can be found on the IEC website at: http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2

6.1.3 IEC 62351-3: Profiles including TCP/IP

Part 3 of the IEC 62351 series provides technical specifications on ensuring the confidentiality, tamper detection, and message level authentication for SCADA and other telecontrol protocols which use TCP/IP as a message transport layer between communicating entities. TCP/IP-based protocols are secured through specification of the messages, procedures, and algorithms of Transport Layer Security (TLS).

Other IEC TC57 standards are expected to use IEC 62351-3 when they implement TCP-IP-based protocols at the Transport Layers; however, those TC57 standards that do not specify Transport Layers, do not include (and do not need to include) normative references to IEC 62351-3.

6.1.4 IEC 62351-4: Profiles including MMS

Part 4 of the IEC 62351 series provides specifications to secure information transferred when using ISO 9506, Manufacturing Message Specification (MMS)-based applications; specifying which procedures, protocol extensions, and algorithms to use in MMS to provide security.

If encryption is not employed, then the specific threats countered in this part include:

- Unauthorized access to information.

If IEC 62351-3 is employed for Transport Layer security, then the specific threats countered in this part include:

- Unauthorized access to information through message level authentication and encryption of the messages, and
- Unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

The following security attack methods are countered:

- Man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism,
- Tamper detection/message integrity: these threats will be countered through the algorithm used to create the authentication mechanism, and
- Replay: this threat will be countered through the use of specialized processing state machines.

6.1.5 IEC 62351-5: Security for IEC 60850-5 and Derivatives

Part 5 of the IEC 62351 series specifies messages, procedures, and algorithms that apply to the operation of all protocols based on/derived from IEC 60870-5, *Telecontrol equipment and systems-Part 5: Transmission protocols.* The focus of this 62351-5 is on the application layer authentication and security-issues that are a result of application layer authentication. While authentication of sources and receivers is considered the most important requirement and confidentiality is not considered important, encryption can be included by combining this standard with other security standards, such as IEC 62351-3, TLS.

If encryption is not employed, then the specific threats countered in this part include:

- Unauthorized access to information.

If IEC 62351-3 is employed for Transport Layer security, then the specific threats countered in this part include:

- Unauthorized access to information through message level authentication and encryption of the messages, and

- Unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

The following security attack methods are countered:

- Man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism,
- Tamper detection/message integrity: these threats will be countered through the algorithm used to create the authentication mechanism, and
- Replay: this threat will be countered through the use of specialized processing state machines.

This standard applies to, but is not limited to:

- IEC 60870-5-101, Companion standard for basic telecontrol tasks,
- IEC 60870-5-102, Companion standard for the transmission of integrated totals in electric power systems,
- IEC 60870-5-103, Companions standard for the informative interface of protection equipment,
- IEC 60870-5-104, Network access for IEC 60870-5-101 using standard transport profiles, and
- DNP3, Distributed Network Protocol (based on IEC 60870-1 through IEC 60870-5 and controlled by the DNP Users Group).

6.1.6 IEC 62351-6: Security for IEC 61850 Profiles

Part 6 of the IEC 62351 series addresses security for IEC 61850 profiles through specification of messages, procedures, and algorithms. IEC 61850 specifies a number of different profiles which have different constraints, performance requirements, and security needs, but the primary requirement is for authentication of sources of data, receivers of data, and data integrity. Therefore, different security options are specified.

For instances, the GOOSE profile is used primarily for very high speed, short latency (<4 ms latency), high availability interactions over dedicated communication channels between protective relays. In this environment, authentication is vital, but confidentiality (implying the encryption of data) is not needed and actually should not be used, due to the tight latency constraints and the need for protective relays to operate with very high availability. The concern is that encryption may hinder rapid response.

The Sampled Measured Values (SMV) profile is for streaming sensor data over a dedicated communication channel. For this profile, authentication is necessary, but encryption is not needed.

The ACSI profile is used primarily to monitor and control field equipment over networks with less stringent performance requirements, so that providing additional security is feasible. In particular, Part 3 and Part 4 are specified.

If encryption is not employed, then the specific threats countered in this part include:

- Unauthorized access to information.

If IEC 62351-3 is employed for Transport Layer security, then the specific threats countered in this part include:

- Unauthorized access to information through message level authentication and encryption of the messages, and
- Unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

The following security attack methods are countered:

- Man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism,
- Tamper detection/message integrity: these threats will be countered through the algorithm used to create the authentication mechanism, and
- Replay: this threat will be countered through the use of specialized processing state machines.

This standard applies to, but is not limited to:

- IEC 61850-8-1, Communication networks and systems in substations-Part 8-1: Specific Communication Service Mapping (SCSM)-Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3,
- IEC 61850-8-2, Communication networks and systems in substations-Part 8-2: Specific Communication Service Mapping (SCSM)-Sampled values over ISO/IEC 8802-3, and
- IEC 61850-6, Communication networks and systems in substations-Part 6: Configuration description language for communication in electrical substations related to IEDs.

6.1.7 IEC 62351-7: Security through Network and System Management

Part 7 of the IEC 62351 series provides an abstract model of network and system data elements that should be monitored and controlled. Its focus is network and system management, one area among many possible areas of end-to-end information security. The primary focus is the enhancement of overall management of the communications networks supporting power system operations, by specifying monitoring and control of communication networks and systems. Intrusion detection and intrusion prevention are addressed.

6.2 IEC 62351-1: Summary of Cyber Security Content

6.2.1 Does the standard address cyber security? If not, should it?

Yes, the standard addresses cyber security as an introduction to parts 2-7 by introducing the reader to different areas of information security as it applies to power system operations. IEC 62351-1 also contains a general discussion of security threats and attack methods.

6.2.2 What aspects of cyber security does the standard address and how well (correctly) does it do so?

62351-1 acts as an introduction to the 62351 series, cyber security concepts, and terminology. This clause does not include or address specific requirements, rather, is intended to provide security awareness. Examples of security requirements are provided.

The applicable NISTIR 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Awareness and Training (SG.AT)	SG.AT-2, Security Awareness

6.2.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

IEC 62351-1 acts as an introduction to the 62351 series. There is a discussion about overarching security issues that the series addresses, but no specific requirements. Specific requirements relevant to later parts in the series are addressed in that respective standard.

Some issues raised by a NIST reviewer include the following***: (When IEC 62351-1 is updated, these comments should be presented to IEC TC57 WG15.)***

- ***In clause 5.2.3.6, Viruses and Worms, the reference to the term "man-in-the middle" attack implies that it is a virus which is not necessarily accurate.***
- ***Further clarification is required in Clause 5.3.1, Security Requirements. The four security requirements, confidentiality, integrity, availability and non-repudiation or accountability should not be classified as requirements, rather as security objectives. Also, from the NIST perspective, the fourth "requirement," non-repudiation, is covered under integrity and does not need to be listed as a separate "requirement."***
- ***Clause 5.3.2 – 5.3.4, Security Threats, Security Vulnerabilities, and Security Attacks, the concept of threats, vulnerabilities, and attacks need to be more clearly explained***
- ***An overall suggestion was to look to NIST Special Publications (SPs) for further guidance, clarification, and consistency. Relevant NIST SPs include: 800-53, Appendix I, 800-18, 800-37 Rev.1, and coming soon, 800-39 and 800-30. There is an issue with consistency of terminology and clarity throughout the standard, for example, use of the terms "requirements vs. objectives," "threats," "countermeasures," and "requirements."***

6.2.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

Part 1 will be updated within the next 2-3 years. Comments will be used at that time to improve the discussion of security in this informative Part.

6.2.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed.

The following standards are normative as described in 62351-1:

- IEC 60870-5 (all parts), *Telecontrol equipment and systems – Part 5: Transmission protocols*
- IEC 60870-6 (all parts), *Telecontrol equipment and systems-Part 5: Telecontrol protocols compatible with ISO standards and ITU-T recommendations*
- IEC 61850 (all parts), Communication networks and systems in substations

6.3 IEC 62351-2: Summary of Cyber Security Content

6.3.1 Does the standard address cyber security? If not, should it?

Yes, IEC 62351-2 provides a cyber security glossary, but contains no security requirements.

6.3.2 What aspects of cyber security does the standard address, and how well (correctly) does it do so?

IEC 62351-2 contains no security requirements; it provides definitions for common cyber security terminology.

6.3.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

IEC 62351-2 contains no security requirements; it provides definitions for common cyber security terminology.

6.3.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

IEC 62351-2 contains no security requirements; it provides definitions for common cyber security terminology.

6.3.5 List any references to other standards and whether they are normative or informative.

None

6.4 IEC 62351-3: Summary of Cyber Security Content

6.4.1 Does the standard address cyber security? If not, should it?

The standard addresses cyber security for protocols using the TCP/IP as a message transport layer by specifying how to ensure confidentiality, tamper detection, and

message layer authentication for SCADA and telecontrol protocols. This standard covers security for the Network and Transport Layers of the OSI communications stack.

6.4.2 What aspects of cyber security does the standard address, and how well (correctly) does it do so?

Specific cyber security issues addressed by this standard include:

- Operational requirements affecting the use of TLS in the telecontrol environment
  - Duration of TCP/IP connection (security must be maintained)
  - Need to provide confidentiality for IEC/TC 57 connections with longer durations through a transparent mechanism for encryption key re-negotiation
  - Interoperability between implementations (standard specifies that referring standards must specify at least one common cipher suite and a set of TLS parameters that allow interoperability)
- A description of security threats and attack methods countered
  - Security threats that can be countered through message level authentication and encryption of messages
    - Unauthorized access to information
    - Unauthorized modification (tampering) or theft of information
  - Attack methods that can be countered through implementation of specification and recommendations
    - Man-in-the middle: use of message authentication code mechanism specified
    - Replay: use of specialized state machines specified in RFC 2246, RFC 2712, and RFC 3268
    - Eavesdropping: use of encryption
- Mandatory requirements listed include:
  - Deprecation of non-encryption cipher suites
  - Negotiation of versions
  - Cipher negotiation
  - Message authentication code
  - Certificate support
    - Multiple certificate authorities (CAs)
    - Certificate size
    - Certificate exchange
    - Certificate comparison
      - Verification based upon CA
      - Verification based upon individual certificates
      - Certificate revocation
      - Expired certificates
      - Signing
      - Key exchange
      - Co-existence with non-secure protocol traffic

The applicable NISTIR 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Smart Grid Information System and Communications Protection (SG.SC)	SG.SC-8, Communication Integrity SG.SC-9, Communication Confidentiality SG.SC-12, Use of Validated cryptography SG.SC-15 Public Key Infrastructure Certificates SG.SC-18, System connections
Identification and Authentication (SG.IA)	SG.IA-4, User Identification and Authentication SG.IA-5, Device Identification and Authentication

6.4.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Within the limits of its scope, there are no gaps, assuming the use of current versions for the referenced protocols. Cryptography is not directly included in the standard although IEC 62351-3 lists that weak TLS cipher suites that "shall not be used."

The mechanisms that are specified as the minimum are somewhat out of date. While the specified mechanisms were appropriate at the time the standard was originally published, newer or stronger mechanisms are now required due to new attacks and advances in computing power available to attackers.

It is recommended that IEC 62351-3 be updated to include the following:

- ***The document should reference RFC 5746, "Transport Layer Security (TLS) Renegotiation Indication Extension". This specification corrects a security flaw in the renegotiation process, which is important in this specification.***
- ***The specification requires support for 1024 bit RSA and DH keys, but the minimum maximum should be raised to 2048.***
- ***The document specifies SHA-1 for all cipher suites; SHA-256 based cipher suites should be specified as options (if not specified as the mandatory cipher suite).***
- ***The specification references a number of RFCs that have been updated or made obsolete. Most importantly, RFC 2246 TLS 1.0 has been made obsolete by RFC TLS 1.2. Another example is RFC 3280 (PKIX Certificate and CRL Profile), which has been made obsolete by RFC 5280. The newer specifications include a number of important enhancements and clarifications.***

6.4.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

Part 3 will be updated within the next 2-3 years.

6.4.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed.

The following references are normative as described in 62351-3:

- IEC 62351-1, *Power systems management and associated information exchange – data and communications security-Part 1: Communication network and system security-introduction to security issues*
- IEC 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*
- RFC 2246:1999, *The TLS Protocol Version 1.0*
- RFC 2712:1999*, Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*
- RFC 3268, 2002, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*
- RFC 3280, 2002, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

6.5 IEC 62351-4: Summary of Cyber Security Content

6.5.1 Does the standard address cyber security? If not, should it?

This standard covers security for the application and transport layers of the OSI communications stack for MMS, specifically addressing procedures, protocol extensions, and algorithms to facilitate securing ISO 9506-Manufacturing Message Specification-based applications. Of the IEC TC 57 standards, IEC 61850-8-1 and IEC 60870-6 use MMS.

6.5.2 What aspects of cyber security does the standard address and how well (correctly) does it do so?

IEC 62351-4 addresses tamper detection and message level authentication.

The applicable NISTIR 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Smart Grid Information System and Communications Protection (SG.SC)	SG.SC-8, Communication Integrity SG.SC-9, Communication Confidentiality SG.SC-12, Use of Validated cryptography SG.SC-18, System connections
Identification and Authentication (SG.IA)	SG.IA-4, User Identification and Authentication SG.IA-5, Device Identification and Authentication
Access Control (SG.AC)	SG.AC-14, Permitted Actions without Authentication

6.5.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Within the limits of its scope, there are no gaps. It addresses tamper detection and message level authentication. Cryptography, however, is not directly included in the standard, but pointers to RSA and TLS are included in the normative references and it identifies cryptographic cipher suites. As noted by a NIST reviewer, the specification references appropriately strong cryptography, TLS_DH_DSS_WITH_AES_256_SHA, as mandatory to implement. However, the specification also allows as a minimum the use of

relatively weak cryptography (i.e., TLS_RSA_WITH_RC4_128_). The specification does not include newer cipher suites with SHA256; these cipher suites might be stronger than currently needed, but should be specified to enable cryptographic migration.

It is recommended that IEC 62351-4 be updated to include new cipher suites with SHA256 to enable cryptographic migration.

6.5.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

Part 4 will be updated within the next 2-3 years.

6.5.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed.

The following standards are normative as described in 62351-4:

- IEC 60870-6 (all parts), *Telecontrol equipment and systems*
- IEC 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*
- IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
- ISO 9506 (all parts*), Industrial automation systems – Manufacturing Message Specification*
- RFC 1006, *ISO Transport Service on top of the TCP Version: 3*
- RFC 2313, *PKCS #1: RSA Encryption Version 1.5*
- RFC 2246, *The TLS Protocol, Version 1.0*
- RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*

The following standards are informative as described in 62351-4:

- ISO/IEC 9594-8:2005 *ITU-T Recommendation X.509:2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

6.6 IEC 62351-5: Summary of Cyber Security Content

6.6.1 Does the standard address cyber security? If not, should it?

IEC 62351-5 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 60870-5, including DNP3. This standard focuses only on application layer authentication and security issues arising from such authentication, and therefore does not address confidentiality. It provides authentication through challenge/response mechanisms using HMAC and secret key methods, to avoid compute and/or media intensive cryptographic calculations.

6.6.2 What aspects of cyber security does the standard address and how well (correctly) does it do so?

IEC 62351-4 addresses message level authentication for all protocols based on/derived from IEC 60870-5, including DNP3.

The applicable NISTIR 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Smart Grid Information System and Communications Protection (SG.SC)	SG.SC-8, Communication Integrity SG.SC-9, Communication Confidentiality SG.SC-15, Public Key Infrastructure Certificates SG.SC-12, Use of Validated cryptography SG.SC-18, System connections
Identification and Authentication (SG.IA)	SG.IA-4, User Identification and Authentication SG.IA-5, Device Identification and Authentication
Access Control (SG.AC)	SG.AC-14, Permitted Actions without Authentication

6.6.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Several security issues were discovered in a recent cyber security review of DNP 3.0 Secure Authentication Supplement V2.0 (which was based on and nearly identical to IEC 62351-5). Secure Authentication Supplement V3.0 addresses most of these issues, and will be reflected in an amendment to IEC 62351-5.

Cryptography is not specified, but it is recommended that HMAC with SHA-1 (160 bits) and AES-128 encryption be included in this standard.

6.6.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

IEC 62351-5 is being updated to reflect the issues addressed above. The timeline for completion is unknown at this time. A detailed cryptography review for this standard has been conducted and a report may be requested from EPRI.

6.6.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed.

The following standards are normative as described in 62351-5:

- IEC 60870-5-101, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

- IEC 60870-5-102, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 102: Companion standard for the transmission of integrated totals in electric power systems*
- IEC 60870-5-103, *Telecontrol equipment and systems – Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment*
- IEC 60870-5-104, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*
- IEC/TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*
- IEC/TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*
- IEC/TS 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
- ISO/IEC 9798-4*, Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*
- FIPS 186-2, *Digital Signature Standard (DSS)*
- FIPS 198-1, *The Keyed-Hash Message Authentication Code*
- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 3174, *Secure Hash Algorithm (SHA-1)*
- RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*
- RFC 3629, *UTF-8, a transformation format of ISO 10646*

The following standards are informative as described in 62351-5:

- FIPS 197, *Advanced Encryption Standard (AES)*

6.7 IEC 62351-6: Summary of Cyber Security Content

6.7.1 Does the standard address cyber security? If not, should it?

This part of IEC 62351 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 61850, Parts 6, 8-1, and 9-2. It is expected to be used in conjunction (as appropriate) with IEC 62351-3 (TLS) and IEC 62351-4 (MMS).

6.7.2 What aspects of cyber security does the standard address, and how well (correctly) does it do so?

IEC 62351-6 addresses tamper detection (integrity), information theft, man-in-the-middle, replay, and message level authentication. However, it is being amended to reflect results from vendor implementations that discovered some inconsistencies that require the standard to be updated.

The applicable NISTIR 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Smart Grid Information System and Communications Protection (SG.SC)	SG.SC-8, Communication Integrity SG.SC-9, Communication Confidentiality SG.SC-12, Use of Validated cryptography

	SG.SC-15, Public Key Infrastructure Certificates SG.SC-18, System connections
Identification and Authentication (SG.IA)	SG.IA-4, User Identification and Authentication SG.IA-5, Device Identification and Authentication
Access Control (SG.AC)	SG.AC-14, Permitted Actions without Authentication

6.7.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Several security issues were discovered in a recent cyber security review of DNP 3.0 Secure Authentication Supplement V2.0 (which was based on and nearly identical to IEC 62351-5). Secure Authentication Supplement V3.0 addresses most of these issues. Cryptography is not specified, but HMAC with SHA-1 (160 bits) and AES-128 encryption should be included in this standard.

6.7.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

IEC 62351-6 is expected to be updated to reflect results from vendor implementations that discovered inconsistencies. The timeline for completion is unknown at this time.

A review of the cryptography has been undertaken, and the document is being amended to cover SHA-256 MAC, RSA 1024 bit signatures and AES-128 used for an combination of confidentiality, integrity, and authentication.

6.7.5 List any references to other standards and whether they are normative or informative.

A cyber security review was not conducted on each standard or document listed below due to the large amount listed. As additional standards are reviewed, many of the standards listed below will be assessed

The following standards are normative as described in 62351-6:

- IEC 61850 (all parts*), Communication networks and systems in substations*
- IEC 61850-6*, Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*
- EC 61850-8-1, *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*
- IEC 61850-9-1, *Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link*
- IEC 61850-9-2*, Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

- IEC 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*
- IEC 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*
- IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*
- ISO 9506 (all parts), *Industrial automation systems – Manufacturing Message Specification*
- ISO/IEC 8802-3*, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*
- ISO/IEC 13239, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures*
- RFC 2030*, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*
- RFC 2313, *PKCS #1: RSA Encryption Version 1.5*
- RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*
- RFC 4634, *US Secure Hash Algorithms (SHA and HMAC-SHA)*

The following standards are normative as described in 62351-6:

- IEEE Std. 802.1Q-2003, *Virtual Bridged Local Area Networks*

6.8 IEC 62351-7: Summary of Cyber Security Content

6.8.1 Does the standard address cyber security? If not, should it?

Using the concepts developed in the IETF Simple Network Management Protocol (SNMP) standards for network management, IEC 62351-7 defines Network and System Management (NSM) abstract data object models that are specific to power system operations. These NSM data objects, mapped to appropriate protocols, will be used to monitor networks and systems, detect possible security intrusions, and to manage the performance and reliability of the information infrastructure.

6.8.2 What aspects of cyber security does the standard address, and how well (correctly) does it do so?

The applicable NISTIR 7628, *Guidelines to Smart Grid Cyber Security*, families and requirements are:

Applicable NISTIR Family	Applicable NISTIR Requirement
Physical and Environmental Security (SG.PE)	SG.PE-4, Monitoring Physical Access
Configuration Management (SG.CM)	SG-CM-2, Baseline Configuration SG.CM-3, Configuration Change Control SG.CM-4, Monitoring Configuration Changes SG.CM-6, Configuration Settings SG.CM-8, Component Inventory
Smart Grid Information System and Communication Protection (SG.SC)	SG.SC-5, Denial-of-Service Protection SG.SC-6, Resource Priority

	SG.SC-7, Boundary Protection SG.SC-8, Communication Integrity SG.SC-22, Fail in Known State
Incident Response (SG.IR)	SG.IR-5, Incident Handling SG.IR-6, Incident Monitoring SG.IR-7, Incident Reporting
Smart Grid Information System and Information Integrity (SG.SI)	SG.SI-4, Smart Grid Information System Monitoring Tools and Techniques SG.SI-5, Security Alerts and Advisories SG.SI-6, Security Functionality Verification SG.SI-7, Software and Information Integrity SG.SI-8, Information Input Validation SG.SI-9, Error Handling
Audit and Accountability (SG.AU)	SG.AU-6, Audit Monitoring, Analysis, and Reporting SG.AU-8, Time Stamps

6.8.3 What aspects of cyber security does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Within the limits of its scope of abstract NSM data objects, there are no gaps. This specification defines abstract network security management objects which will be mapped to some communications protocol. These communication protocols are not specified in the standard in order to permit the mapping to different network management protocols for different implementations, such as the IETF's SNMP or ISO's CMIP or IEC 61850. A more recent possible protocol is the currently emerging IETF NetConf protocol.

However, the scope does not address one issue related to implementing these abstract NSM data objects which is that the security requirements are not defined for the communications for exchanging these objects (once they are mapped to a communications protocol). Although it is not necessary for this specification to select a single network management protocol, it is critical to discuss the different levels of security requirements for that communication. In some cases, it only will be important to authenticate the source. In other cases, the NSM may require encryption because it contains information that could be used by an attacker. Regardless, the determination of the sensitivity of NSM information will be implementation-specific, and cannot be specified in an abstract model.

It is recommended that IEC 62351-7 be updated to include the need to define the security requirements for exchanging the NSM data objects.

6.8.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

This standard was released in 2010 and is not due for updates in the near future.

6.8.5 List any references to other standards and whether they are normative or informative.

The following standards are normative as described in 62351-7:

- IEC/TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*